UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO

UNITED STATES OF AMERICA Plaintiffs, vs. BRIAN E. SAWYER Defendant.	CASE NO. 5:11-CR-00139 OPINION & ORDER [Resolving Doc. No. 23]

JAMES S. GWIN, UNITED STATES DISTRICT JUDGE:

Defendant Brian E. Sawyer moves the Court to suppress evidence found during an allegedly illegal search and seizure of the Defendant's computer files. [Doc. 23.] The United States of America opposes the motion. [Doc. 24.] For the following reasons, the Court **DENIES** the Defendant's motion to suppress.

I. Background

In this case, the United States charges the Defendant with possession and distribution of child pornography, in violation of 18 U.S.C. § 2252(a)(2) and 18 U.S.C. § 2252A(a). The government bases its charges on evidence found on the Defendant's computer, which was seized during the execution of a search warrant on March 4, 2011. [Doc. 23-1 at 2-3.] The warrant was based upon information obtained as a result of the Defendant Sawyer's peer to peer file sharing. [*Id.* at 2-3.]

The Defendant used a "closed" peer-to-peer file sharing program called GigaTribe. [*Id.* at

1.] Normally, peer-to-peer file sharing programs, such as LimeWire or Kazaa, allow anyone using the same software to view and download files from the shared folder on any other user's computer, without special permission. Thus, in these "open" file sharing programs, any files stored in the shared folder on a user's hard drive are visible and may be downloaded by any other person using that same program.

The Defendant used a program called GigaTribe that is slightly different from these "open" programs. With GigaTribe, a user's files are not automatically made publicly available to all other users; instead, users may view and download files only after receiving specific authorization. [*Id.* at 1.] Consent to view and download files on GigaTribe is given when a user adds another user to his or her private list of so-called "friends." [*Id.* at 1.] GigaTribe users may become "friends" with other users through an electronic invitation; acceptance of this invitation allows the "friends" to directly browse and download files that are stored on each other's computers over the internet. [*Id.* at 1.] Individuals using the program select specified folders on their computer that they wish to share, and "friends" can browse, search, and download any of the files stored in those folders. [*Id.* at 1.] GigaTribe also features a chat function that allows users to communicate with each other. [*Id.* at 2.]

At the time of the events in question, the Defendant's GigaTribe username was "happyb." [*Id.* at 2.] While using his "happyb" username, the Defendant became online friends with another user, "SB," allowing the two accounts to access each other's shared folders to browse and download files. [*Id.* at 2.] Agent Couch previously obtained written consent from the user in control of the of the "SB" username to use that account for "any purpose relating to an official investigation by the above law enforcement authority [FBI], including (but not limited to) sending and receiving e-mail

or conducting any other electronic communications, accessing stored information, and using and disclosing such communications or information." [Doc. 23-3.] On February 22, 2011, Special Agent Barry Couch of the FBI ("Agent Couch") logged into the GigaTribe network using the "SB" user name, viewed the Defendant's shared file list, and downloaded twenty-eight images of child pornography. [*Id.* at 2.] While downloading the images, Agent Couch and the Defendant, still using the "happyb" and "SB" usernames, engaged in a private chat about sexual contact with minors. [*Id.* at 2.]

During the download process, Agent Couch ascertained the internet protocol (IP) address for the Defendant's internet connection; the Defendant's physical address was later obtained through a subpoena from Time Warner Cable. [Doc. 23-1 at 2; Doc. 1-1.] Based upon this information, the FBI obtained a search warrant for Defendant Sawyer's home at 230 Superior Street, Louisville, Ohio, that was executed on March 4, 2011. [Doc. 23-1 at 2-3.] During the search, Defendant Sawyer's computer was seized and Sawyer was also interrogated for several hours. [*Id.*]

On April 6, 2011, a federal grand jury indicted the Defendant on one count of receipt and distribution of images of child pornography in violation of of 18 U.S.C. § 2252(a)(2) and one count of possession of a computer containing child pornography in violation of of 18 U.S.C. § 2252A(a). [Doc. 7.] The Defendant now moves the Court to suppress all evidence seized when Agent Couch logged onto the "SB" user name and downloaded files on February 22, 2011, as well as any evidence later seized as a result of that search and seizure, including the Defendant's computer. [Doc. 23.]

II. Analysis

The Fourth Amendment protects individuals against "unreasonable searches and seizures" by the government and protects privacy interests where an individual has a reasonable expectation

of privacy. *Smith v. Maryland*, 442 U.S. 735, 740 (1979). An expectation of privacy is protected by the Fourth Amendment where (1) an individual has exhibited a subjective expectation of privacy, and (2) that expectation of privacy is one that "'society is prepared to recognize as reasonable.'" *Id.* (quoting *Katz v. United States*, 389 U.S. 347, 516 (1967) (Harlan, J., concurring)). In areas where an individual has a legitimate privacy interest, the Fourth Amendment prohibits warrantless searches of an individual's home or possessions, subject to only limited exceptions. *Illinois v. Rodriguez*, 497 U.S. 177, 181 (1990). "Where valid consent is given, [however,] a search is permissible under the Fourth Amendment[,] even without a warrant or probable cause." *United States v. Morgan*, 435 F.3d 660, 663 (6th Cir. 2006) (citing *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973)). Valid consent may be given not only by the defendant, but also by "a third party who possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected." *United States v. Matlock*, 415 U.S. 164, 171 (1974). Generally, any evidence obtained in violation of the Fourth Amendment must be suppressed, as well as any evidence seized subsequent to that illegal investigation as "fruits of the poisonous tree." *Wong Sun v. United States*, 371 U.S. 471, 487-88 (1963).

First, the Court must determine whether Defendant Sawyer has a Fourth Amendment privacy interest in the materials stored on his computer that were shared on GigaTribe. A general consensus has formed among courts that an individual does not have a Fourth Amendment privacy interest in information made available on a public peer to peer filing sharing programs, such as LimeWire or Kazaa, since their expectation of privacy in that shared information is not objectively reasonable. *United States v. Borowy*, 595 F.3d 1045, 1047-49 (9th Cir. 2010) (denying motion to suppress and finding that a defendant lacked a reasonable expectation of privacy over files that were made

publicly available); *United States v. Stults*, 575 F.3d 834, 841-43 (8th Cir. 2009) (same); *United States v. Ganoe*, 538 F.3d 1117, 1128 (9th Cir. 2008) (same); *United States v. Brese*, 2008 WL 1376269, at *2 (W.D. Okla. Apr. 9, 2008) (same); *United States v. Meysenburg*, 2009 WL 1090664, at *2 (D. Neb. Apr. 22, 2009) (same); *State v. Thornton*, 2009 WL 3090409, at *2-3 (Ohio Ct. App. Sept. 22, 2009) (same). Indeed, a person who grants the public access to folders on his computer cannot be said to have an objectively reasonable expectation of privacy in those folders, as any member of the public using that program has free and unfettered access to them. *Ganoe*, 538 F.3d at 1127.

In the current case, however, where a person shares files over a "closed" network – in which only pre-approved friends have access – an expectation of privacy is somewhat more reasonable. Unlike in an open program, where any user can see and download the files, Defendant Sawyer's files were only visible to his "friends." [Doc. 23-1 at 1-3.] Nonetheless, despite the program affording some greater degree of privacy, the rationale of the decisions analyzing open file sharing programs is still persuasive here and the Court finds that Sawyer did not have an objectively reasonable expectation of privacy in the files that were shared over GigaTribe. *United States v. Ladeau*, 2010 WL 1427523, at *1-5 (D. Mass. Apr. 7, 2010) (holding an individual using GigaTribe has no reasonable expectation of privacy in the information that they share). Once Defendant Sawyer granted his "friends" access to his files, he had no control over the manner in which his friends used that access. *Id.* The Supreme Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith*, 442 U.S. at 743-44; *see also United States v. White*, 401 U.S. 745, 752 (1971) ("Inescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to the police."); *see also*

Hoffa v. United States, 385 U.S. 293, 302 (1966) ("Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."). Defendant Sawyer voluntarily made his files available to all of his "friends" and he also bore the risk that those "friends" might turn the files over to law enforcement. *United States v. Meriwether*, 917 F.2d 955, 958 (6th Cir. 1990) (finding no reasonable expectation of privacy in information sent to pager even though sender did not know Government had pager). The Court, therefore, finds that the Defendant did not have an objectively reasonable expectation of privacy in the information that he shared over GigaTribe and that Agent Couch's activities on the "SB" username did not implicate the Fourth Amendment. *See United States v. Haffner*, 2010 WL 5296920, at *5-6 (M.D. Fla Aug. 31, 2010) (finding that a defendant has no legitimate expectation of privacy in messages and images transmitted over internet).

Moreover, even if Defendant Sawyer possessed a privacy interest in the shared files stored on his computer, the Court finds that consent was given to search those files. First, Defendant Sawyer himself directly consented to the February 22 downloads. Simply because the government obtained access to these files through use of a ruse does not render the consent involuntary. Rather, "it is well established that an undercover officer may gain entrance [to a home] by misrepresenting his identity and may gather evidence while there." *United States v. Pollard*, 215 F.3d 643, 649 (6th Cir. 2000). For example, in *United States v. Lord*, the Sixth Circuit found consent voluntary where government agents posing as real estate investors gained access to an individual's bedroom and bedroom closet. 230 F. App'x 511, 514 (6th Cir. 2007). Here, the Defendant freely granted the username "SB," which Agent Couch was using at the time, access to his files, believing that Couch

wanted to download child pornography, even going as far as to discuss previous sexual contact with minors during the download process.[1/] [Doc. 23-1.] It is difficult to see how the consent directly given to Agent Couch while using the "SB" account was not made voluntarily.

Second, as to third party consent, the owner of the "SB" account also validly consented to Agent Couch searching the shared folder on Defendant Sawyer's computer. It is well accepted that a third party with authority or control over property subject to a search may grant law enforcement consent to search that property. *Morgan*, 435 F.3d at 663. For example, a third party with access to a home computer may consent to a police search of the files on that computer. *Id.* at 664. However, where certain files on the computer are password protected or where the consenting third party otherwise lacks access to them, the third party generally has no authority to consent to a police search of those locked files. *United States v. Andrus*, 483 F.3d 711, 718-19 (10th Cir. 2007); Trulock v. French, 275 F.3d 391, 403 (4th Cir. 2001) (finding Fourth Amendment rights were violated where FBI searched password-protected computer files based on his roommate's consent because roommate did not have access to password-protected files); *United States v. Trejo*, 2010 WL 940036, at *3-11 (E.D. Mich. Mar. 12, 2010) (finding effective third-party consent given to computer search where user had access to files and folders); *United States v. Albertson*, 2006 WL 3613776, at *4-9 (M.D. Pa. Dec. 11, 2006) (holding third party could consent to search of computer where she had access to computer).

Here, by becoming "friends" with "SB," Defendant Sawyer granted the "SB" username the

---

[1/] This case is easily distinguishable from *United States v. Hardin*, 539 F.3d 406 (6th Cir. 2008). In that case, the Sixth Circuit found that consent was not validly obtained where government agents entered the defendant's apartment while pretending to be maintenance workers who needed to fix a water leak. The consent was not voluntary in that case because the defendant, believing that there was an emergency leak in his apartment, did not have a choice to deny the "maintenance workers" entry. *Id.* at 425. Here, it is not possible to argue that Defendant Sawyer believed that he had no choice but to allow "SB" to download files of child pornography.

authority to access any files or folders designated as shared. The owner of the "SB" name then voluntarily consented to Agent Couch using that username to access the shared folders and files on Sawyer's computer. [Doc. 23-3.] It makes little difference that "SB" was granted authority to access and download the files on the computer over the internet, rather than through a grant of physical access to the computer actually storing those files, particularly since Agent Couch only accessed the files remotely over the internet. As such, the Court finds that even if the Defendant has a Fourth Amendment privacy interest in the shared files on his computer, that the user in control of the "SB" gave effective third-party consent to a police search of those shared files.

For the foregoing reasons, the Court **DENIES** the Defendant's motion to suppress.

IT IS SO ORDERED.

Dated: May 25, 2011

s/ *James S. Gwin*
JAMES S. GWIN
UNITED STATES DISTRICT JUDGE